UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,128	10/31/2003	Simon C. Chu	RPS920030115US3	8930

7590 07/05/2006

IBM Corporation
Intellectual Property Law Dept. 9CCA/B002
P.O. Box 12195
Res. Tri. Park, NC 27709

EXAMINER	
STOYNOV, STEFAN	

ART UNIT	PAPER NUMBER
2116	

DATE MAILED: 07/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Interview Summary	Application No.	Applicant(s)	
	10/698,128	CHU ET AL.	
	Examiner	Art Unit	
	Stefan Stoynov	2116	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Stefan Stoynov*.

(2) *Lynne Browne*.

(3) *James E. Boice (Reg. No. 44,545)*.

(4)_____.

Date of Interview: *21 June 2006*.

Type: a)☒ Telephonic b)☐ Video Conference
c)☐ Personal [copy given to: 1)☐ applicant 2)☐ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☒ No.
If Yes, brief description: _____.

Claim(s) discussed: *1 and 3*.

Identification of prior art discussed: *US 2004/0193876 and US 6,314,520*.

Agreement with respect to the claims f)☐ was reached. g)☐ was not reached. h)☒ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *See attached Interview Agenda (11 pages) for discussion details. No agreement was reached for claim 3. Regarding claim 1, the examiner acknowledged that the proposed amendment overcomes the prior art of record*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

LYNNE H. BROWNE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

Examiner's signature, if required

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)
In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

DILLON & YUDELL LLP

ATTORNEYS AT LAW

USPTO FACSIMILE TRANSMITTAL SHEET

TO:	FROM:
Examiner Stefan Stoynov	James E. Boice, Reg. No. 44,545
ORGANIZATION:	DATE:
US Patent and Trademark Office	June 19, 2006
ART UNIT:	TOTAL NO. OF PAGES INCLUDING COVER:
2116	11
FAX NUMBER:	APPLICATION SERIAL NOS:
571.273.4236	10/698,207 10/675,624 10/675,776 10/698,128 10/698,208 10/674,838
ENCLOSED:	ATTORNEY DOCKET NO:
Proposed agenda	RPS920030115US4 RPS920030115US1 RPS920030115US2 RPS920030115US3 RPS920030114US2 RPS920030114US1

☒ URGENT ☐ FOR REVIEW ☐ PLEASE COMMENT ☐ PLEASE REPLY ☐ PLEASE RECYCLE

NOTES/COMMENTS:

Dear Examiner Stoynov:

Thank you for agreeing to conduct a teleconference regarding the above captioned patent applications on Wednesday, June 21, 2006 at 2:00 EDT. I will call Examiner Browne's office (571.272.3670) at that time.

8911 N. CAPITAL OF TEXAS HWY., SUITE 2110, AUSTIN, TEXAS 78759
512.343.6116 (V) • 512.343.6446 (F) • DILLONYUDELL.COM

Attached is a new agenda, which discusses applications 10/698,208 and 10/674,838 as well. (Although not cited, these applications are on similar technology as that found in applications 10/675,776, 10/698,128, 10/675,624 and 10/698,207.

If you have any preliminary ideas for amendments that would promote allowance, I would be most appreciative of your input.

Best regards,

Jim Boice
Attorney for Applicants

Agenda for Wednesday, June 21, 2006 at 2:00 EDT.

Application 10/698,207

Claim 1. "under the control of a remote supervisory computer connected via a hyper-secure link to a client computer, storing a list of trusted configuration servers in the client computer"

In other words, this element says that the list of trusted configuration servers in the client computer is stored by a remote supervisory computer.

Zimmer fails to disclose storing a list of trusted configuration servers in the client computer. However, at col. 2, lines 30-35, col. 3, liens 6-11, col. 4 line 64 to col. 5, line 2, and col. 5, lines 13-22, *Schell* teaches that a NIC can store addresses of trusted servers, which are compared to the source address of incoming packets.

The limitation that is still not taught or suggested is that of having a remote supervisory computer perform the storage of the list in the client computer. Rather, this storage is part of the initialization that is performed locally by the client computer. As stated at col. 6, lines 8-20:

> "Initialization continues with step 124 wherein the CPU executes the program instructions resident in the NIC BIOS 65 (FIG. 3) to initialize the hardware in the NIC. Following hardware initialization, the CPU downloads the pre-boot modules from the server in step 126 and in step 128, executes these pre-boot modules to perform the identification and authorization function associated with the login process described in FIG. 6. In addition the CPU loads the registers of the NIC's send address confirmation circuitry 66 and the receive address confirmation circuit 88 (FIG. 3) with values stored in the NIC BIOS ROM. In an alternative embodiment, the pre-boot modules may be stored in the NIC BIOS." (emphasis added)

That is, the information as to which server is to be trusted comes NOT from a remote supervisory computer, but from the client computer itself (i.e., from the client computer's NIC BIOS).

Claim 2. "upon a determination that the responding configuration server is not on a list of trusted configuration servers, providing the configuration parameters directly from one of the servers on the list of trusted configuration servers"

Schell is cited for teaching the discarding of packets that are from untrusted locations, and accepting only packets from trusted locations. There is no teaching or suggestion of getting a configuration parameter from a server that is selected from the list of trusted configuration servers. That is, *Schell* examines the source address of incoming packets, while Claim 2 relates to the client computer choosing a server to make a call to. Would the following claim language clarify this?

"~~upon a determination~~ in response to determining that the responding configuration server is not on a list of trusted configuration servers, [[providing]] selecting, by the client computer, ~~the configuration parameters directly from~~ a selected server from one of the servers on the list of trusted configuration servers; and

requesting the configuration parameters from the selected server."

(This feature is supported by Figure 3, blocks 318 and 308).

Agenda for Wednesday, June 21, 2006 at 2:00 EDT.

Applications 10/675,624

This invention provides a solution to the problem of obtaining an IP address from an unauthorized DHCP server.

Claim 3. "upon determining that the responding configuration server is not on the list of trusted configuration servers, generating an alert...of an unauthorized configuration server"

Zimmer is cited at paragraph [0044]. This paragraph talks about sending a message to an administrator if no boot option offers were received. Claim 3 is directed to sending a message to an administrator if the responding configuration server is not on the trusted list. While the client computer may end up in the same condition (not getting a boot), teaching a possible result is not the same as teaching a limitation.

Claim 4. "upon determining that the responding configuration server is not on the list of trusted configuration servers, sending the request for the configuration parameter from the computer to a server from the list of trusted configuration servers."

See discussion above for Claim 2 of Application No. 10/698,207.

Would the following language aid in promoting this claim to allowance?

"[[upon]] in response to determining that the responding configuration server is not on a list of trusted configuration servers, ~~sending the request for the configuration parameter from the computer to a server from the list of trusted configuration servers~~ selecting, by the client computer, a selected server from one of the servers on the list of trusted configuration servers; and

requesting the configuration parameters from the selected server."

Agenda for Wednesday, June 21, 2006 at 2:00 EDT.

Application 10/674,776

This invention addresses the problem of using an unfiltered network boot program.

Claim 1.

As none of the cited art is directed to a remote supervisor controlling the storage of a list of trusted PXE boot program servers, would including the following limitations (as supported in the specification in the summary and paragraph [0017] in application 10/674,776) help? For example, Claim 1 in 10/674,776 would read:

1. A service for managing a network boot of a client computer, the method comprising:

storing a list of trusted Pre-boot eXecution Environment (PXE) boot program servers in an interface service card coupled to a client computer on a network, the interface service card also being coupled to a hyper-secure remote service network that includes a remote supervisor, **wherein the remote supervisor controls the storage of the list of trusted PXE boot program servers in the interface service card**;

broadcasting a request for a boot program from the client computer to a network of PXE boot program servers;

receiving a response to the request for the boot program at the client computer, the response being from a responding boot program server on the network of PXE boot program servers;

comparing an identity of the responding boot program server with the list of trusted PXE boot program servers; and

upon verifying that the responding boot program server is on the list of trusted PXE boot program servers, requesting and downloading onto the client computer a boot program from the responding PXE boot program server.

Claim 3. "upon determining that the responding boot program server is not on the list of trusted boot program servers, generating an alert...of an unauthorized boot program server on the network of boot program servers"

See discussion above for Claim 3 in Application No. 10/675,624. Note also the limitation of the unauthorized server being "on the network of boot program servers."

Agenda for Wednesday, June 21, 2006 at 2:00 EDT.

Application 10/698,128

Claim 1

Similar argument as found above for Claim 1 of Application No. 10/674,776. Thus, Claim 1 for Application 10/698,128 would read:

1. A method for managing a network boot of a client computer, the method comprising:

storing a list of trusted Pre-boot eXecution Environment (PXE) boot program servers in an interface service card coupled to a client computer on a network, the interface service card also being coupled to a hyper-secure remote service network that includes a remote supervisor, **wherein the remote supervisor controls the storage of the list of trusted PXE boot program servers in the interface service card**;

broadcasting a request for a boot program from the client computer to a network of PXE boot program servers;

receiving a response to the request for the boot program at the client computer, the response being from a responding boot program server on the network of PXE boot program servers;

comparing an identity of the responding boot program server with the list of trusted PXE boot program servers; and

upon verifying that the responding boot program server is on the list of trusted PXE boot program servers, requesting and downloading onto the client computer a boot program from the responding PXE boot program server.

Claim 3. "upon determining that the responding boot program server is not on the list of trusted boot program servers, generating an alert...of an unauthorized boot program server on the network"

See discussion above in Claim 3 of Application No. 10/675,624. Note also the limitation of the illegal server being "on the network."

Agenda for Wednesday, June 21, 2006 at 2:00 EDT.

Application No. 10/698,208

Claim 1. "generating an alert to a designated administrator server of a presence of an unauthorized management server on the network of management servers"

Frye is cited at paragraph [0047] for this teaching. However, paragraph [0047] of *Frye* discusses a console monitor, on a PXE server, which shows which client computers are using the PXE server. There is no teaching or suggestion of "an alert" being generated, particularly with regards to "a presence of an unauthorized management server." Furthermore, *Frye* shows client computers being monitored, not management (e.g., PXE) servers.

Claim 2. "an information technology services organization logically oriented between the different types of boot program servers and the server blade"

This feature is described in Figure 4 and paragraph [0026] of the present specification. In brief, a centralized service (such as IBM's Global Services) acts as a clearinghouse/filter for different PXE servers, sending the PXE boot request from the blade server to the appropriate PXE server.

Schell is cited at col. 2, lines 3-11. However, *Schell* is directed to a NIC being programmed to accept packets only from trusted sources (see discussion above). There does not seem to be any suggestion of a service such as IGS that acts as a clearinghouse/filter between the client blade server and the PXE servers.

Claim 3. (new) The method of claim 2, wherein the information technology services organization enables a single Information Technology (IT) service organization **assigned systems manager** to manage various deployment server types, maintain permission lists for each PXE boot program server type, monitor a network for unauthorized DCHP/PXE servers, and shut down network ports of unauthorized DHCP/PXE servers.

Agenda for Wednesday, June 21, 2006 at 2:00 EDT.

Can we discuss proposed new Claim 3? (Support is found in paragraph [0026].)

Agenda for Wednesday, June 21, 2006 at 2:00 EDT.

Application No. 10,674,838

Claim 3. "generating an alert to a designated administrator server of a presence of an unauthorized management server on the network of management servers"

Frye is cited at paragraph [0047] for this teaching. However, paragraph [0047] of *Frye* discusses a console monitor, on a PXE server, which shows which client computers are using the PXE server. There is no teaching or suggestion of "an alert" being generated, particularly with regards to the "presence of an unauthorized management server on the network of management servers." Furthermore, *Frye* shows client computers being monitored, not management (e.g., PXE) servers.

Schell is also cited at col. 5, lines 20-22. However, this passage only describes how packets from untrusted locations are discarded. There is no teaching or suggestion of generating an alert regarding an unauthorized management server.

Claim 7. "an information technology services organization logically oriented between the different types of boot program servers and the server blade"

This feature is described in Figure 4 and paragraph [0026] of the present specification. In brief, a centralized service (such as IBM's Global Services) acts as a clearinghouse/filter for different PXE servers, sending the PXE boot request from the blade server to the appropriate PXE server.

Schell is cited at col. 2, lines 3-11. As noted above with reference to Application No. 10/698,208, *Schell* is directed to a NIC being programmed to accept packets only from trusted sources (see discussion above). There does not seem to be any suggestion of a service such as IGS that acts as a clearinghouse/filter between the client blade server and the PXE servers.

Frye is also cited at paragraph [0022]. *Frye* teaches a boot server 130 and a target computer 110, but no intermediate "information technology services organization."

Claim 22. (new) The method of claim 7, wherein the information technology services organization enables a single Information Technology (IT) service organization **assigned systems manager** to manage various deployment server types, maintain permission lists for each PXE boot program server type, monitor a network for unauthorized DCHP/PXE servers, and shut down network ports of unauthorized DHCP/PXE servers.

Can we discuss proposed new Claim 22? (Support is found in paragraph [0026].)